BRENTSIDE PRIMARY ACADEMY

Putting Children First

Headteacher: Caroline Crosdale

E-SAFETY POLICY

Created: November 2017 **Updated:** March 2020

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.

"To ignore e-safety issues when implementing the requirements of Every Child Matters could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable."
From: Safeguarding Children in a Digital World. BECTA 2006

WHY IS INTERNET USE IMPORTANT?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

Pupils will use the Internet inside and outside school, and will need to learn how to evaluate Internet information and to take care of their own safety and security.

BACKGROUND / RATIONALE

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy helps to ensure safe and appropriate use. The development and implementation of such a strategy involves all the stakeholders in a child’s education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual’s consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils’ resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Yorkshire and Humberside Grid for Learning including the effective management of content filtering.
- National Education Network standards and specifications

SCOPE OF THE POLICY

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

EDUCATION OF CHILDREN

A progressive planned e-Safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited.

- Key e-Safety messages are reinforced through an assembly and a discrete e-Safety lesson each term, along with Safer Internet Week (February), anti-bullying week (November) and throughout all lessons where appropriate.
- Children are reminded of key e-Safety messages frequently even when they have already been taught them in previous years.
- Children are taught to keep themselves safe online and to be responsible in their use of different technologies as detailed in the Somerset Byte scheme of work.
- Children are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage children to use specific search terms to reduce the likelihood of coming across unsuitable material.
- In lessons where Internet use is pre-planned, children are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in Internet searches. Staff use the agreed search engines.
- Children are taught to be critically aware of the content they access on-line and are guided to validate the accuracy and reliability of information.
- Children are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Children will write class rules and sign this at the beginning of each school year, which will be shared with parents and carers.
- Children are taught how to use the internet before they go on it.
- Children are taught how computers work to increase their understanding of how it can be used to keep them safe and the possible dangers.
- The internet will be used for educational purposes.

EDUCATION AND INFORMATION FOR PARENTS AND CARERS

Parents and carers will be informed about the ways the Internet and technology is used in school. They have a critical role to play in supporting their children with managing e-Safety risks at home reinforcing key messages about e-safety and regulating their home experiences. The school supports parents and carers to do this by:

- Providing clear e-safety guidance information and letters
- Raising awareness through activities planned by children
- Inviting parents to attend activities such as e-safety week, e-safety assemblies or other meeting as appropriate.

INTERNET USE WITHIN SCHOOL

WORLD WIDE WEB

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Headteacher, by recording the incident in an e-Safety Log. The e-Safety Log will be reviewed termly by the e-Safety Co-ordinator.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible.

E-MAIL

- E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school rather than individual addresses.
- Access in school to external personal e-mail accounts is not allowed.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a using outlook.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

SECURITY AND PASSWORDS

Each pupil is issued with a username and password for the purple mash IT system. Parents are also issued with a parental code so they can gain access to the Purple Mash system.

Replacement Usernames and passwords can be obtained from the school office.

SOCIAL NETWORKING

- Social networking Internet sites (such as, MySpace, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.
- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

MOBILE PHONES

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils by permission of the Headteacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the school office by 9.00am and collected at the end of the day.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff should always use the school phone to contact parents.
- Staff including students and visitors are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the teaching day.
- Parents cannot use mobile phones on school trips to take pictures of the children
- On trips staff mobiles are used for emergency only
- Any photographs taken using staff mobile phones are to be emailed to the school and deleted from the phone as soon as possible.

DIGITAL/VIDEO CAMERAS/PHOTOGRAPHS

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will follow the policy set out in this document under ‘Publishing Content’.
- Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.
- The Headteacher or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner
- Staff should use a school camera to capture images. If a mobile phone is used to take pictures the images should be emailed to the school as soon as possible, then deleted from the personal device.
- Photos taken by the school are subject to the Data Protection act.
- A photo consent form has been issued to parents to find out where digital images of each child can and cannot be used. This form is also issued to all new starters

PUBLISHED CONTENT AND THE SCHOOL WEBSITE

The school website is a valuable source of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number.
- Staff and pupils’ personal information will not be published.
- The Headteacher or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully based on the photo consent form completed by parents.
- Pupils’ full names will not be used in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school Website.
- Work will only be published with the permission of the pupil.
- Parents should only upload pictures of their own child/children onto social networking sites.
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

ASSESSING RISK

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

HANDLING E-SAFETY COMPLAINTS

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Any complaint about Headteacher misuse will be referred to the Chair of Governors.
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.